OSINT + ARCO + PROTECCIÓN DE DATOS

MAPA-RD: Exposición y Ruta de Cierre

Así se ve tu entorno digital desde fuera. Esto es lo que hay que cerrar primero.

MAPA-RD identifica exposición real (visible públicamente), prioriza riesgos y entrega una ruta de cierre ejecututable. Incluye base operativa para gestión ARCO y un esquema mensual de control continuo.

Sin auditorías genéricas. Sin promesas vacías.

ACME Corp · Reporte RPT-2026-001 · 2026-01-11

Executive Security Report · Exposición pública · Confidencial

Índice de Riesgo Digital

65

RIESGO CRÍTICO

VECTORES DE VULNERABILIDAD

VEC-001

Exposed Database Credentials

85 MÁXIMO

ACTIVO:
Production Database (AWS RDS)

TIPO:
Cloud Infrastructure

EXPOSICIÓN:
Public Repo Leak

DESCRIPCIÓN DEL EVENTO

Hardcoded credentials for the primary production database were identified in a public GitHub repository (config.js). Determining access logs confirmed unauthorized clone events.

IMPACTO

- Full compromise of customer data (PII).
- Potential total service disruption (Ransomware).
- Severe regulatory fines (GDPR/CCPA).

RUTA DE CIERRE

1. Revoke the exposed AWS IAM credentials immediately.
2. Rotate the database master password.
3. Audit CloudTrail logs for suspicious activities since the commit date.
4. Implement git-secrets to prevent future commits.

VEC-002

Admin Portal without MFA

60 CRÍTICO

ACTIVO: admin.acme.com

TIPO: Web Application

EXPOSICIÓN: Missing Control

DESCRIPCIÓN DEL EVENTO

The administrative panel allows single-factor authentication. Brute-force attacks or credential stuffing could easily compromise an admin account.

IMPACTO

- Unauthorized administrative access.
- Data manipulation or deletion.
- Backdoor installation.

RUTA DE CIERRE

1. Enforce MFA (Time-based OTP) for all admin roles.
2. Restrict access to VPN or trusted IPs only.
3. Implement rate-limiting on the login endpoint.

VEC-003

Outdated SSL Certificate

35 MEDIO

ACTIVO: dev.acme.com

TIPO: Dev Environment

EXPOSICIÓN: Configuration

DESCRIPCIÓN DEL EVENTO

The SSL certificate for the development environment is expired, triggering browser warnings and exposing traffic to interception.

IMPACTO

- Developer workflow disruption.
- Man-in-the-Middle (MitM) risk if used externally.
- Loss of trust validation.

RUTA DE CIERRE

1. Provision a new LetsEncrypt certificate.
2. Automate renewal via Certbot.

ANEXO TÉCNICO

METODOLOGÍA DE RIESGO V1.0 (OFICIAL)

1. Índice de Riesgo del Vector (IRV)

El IRV mide la urgencia y el impacto real de no remediar un vector de vulnerabilidad específico. Se calcula internamente mediante un modelo ponderado de seis dimensiones y se normaliza a una escala centesimal (0-100).

FÓRMULA GENERAL

$$IRV = [\ \Sigma(Componente \times Peso)\ /\ \Sigma(Pesos\_Max)\ ]\ \times 100$$

VARIABLES DEL MODELO

CA — **Criticidad del Activo** — x4

Evalúa la importancia crítica del sistema afectado para la operación del negocio.

ET — **Exposición Temporal** — x3

Determina si el hallazgo es histórico, residual o plenamente vigente.

SE — **Superficie de Exposición** — x3

Mide la facilidad de acceso desde el exterior (Público vs Privado/Interno).

IM — **Impacto Multidimensional** — x4

Suma binaria de impactos confirmados: Legal, Financiero, Operativo y Reputacional.

FE x3

Facilidad de Explotación

Nivel de esfuerzo técnico y recursos requeridos por el atacante.

DV x3

Detectabilidad

Probabilidad de que la explotación pase desapercibida por los sistemas de defensa.

2. Índice de Riesgo Digital (IRD)

El IRD representa el estado global de riesgo de la organización. Es un indicador dinámico derivado exclusivamente de los IRV activos, utilizando un promedio ponderado por severidad.

CÁLCULO PONDERADO

$$IRD = \Sigma(IRV \times Peso\_Severidad) / \Sigma(Pesos\_Severidad)$$

ESCALA DE SEVERIDAD

BAJO	MEDIO	ALTO	CRÍTICO	MÁXIMO
PESO x1	PESO x2	PESO x3	PESO x4	PESO x5